JOURNAL OF NUMBER THEORY 10, 430–450 (1978)

On Differences and Sums of Integers, I

P. ERDÖS AND A. SÁRKÖZY

Mathematical Institute of the Hungarian Academy of Sciences, 1053 Budapest, Realtánoda utca 13–15, Hungary

Communicated by H. Zassenhaus

Received October 13, 1977

A set $\{b_1, b_2, \ldots, b_i\} \subset \{1, 2, \ldots, N\}$ is said to be a difference intersector set if $\{a_1, a_2, \ldots, a_s\} \subset \{1, 2, \ldots, N\}$, $j > \epsilon N$ imply the solvability of the equation $a_x - a_y = b'$; the notion of sum intersector set is defined similarly. The authors prove two general theorems saying that if a set $\{b_1, b_2, \ldots, b_i\}$ is well distributed simultaneously among and within all residue classes of small moduli then it must be both difference and sum intersector set. They apply these theorems to investigate the solvability of the equations $(a_x - a_y/p) = +1$, $(a_u - a_v/p) = -1$, $(a_r + a_s/p) = +1$, $(a_t + a_z/p) = -1$ (where (a/p) denotes the Legendre symbol) and to show that "almost all" sets form both difference and sum intersector sets.

1

Throughout this paper, we use the following notations:

$c_1, c_2, \ldots$ will denote positive absolute constants. We write $e^x = \exp(x)$. For real α, we put $e(\alpha) = e^{2\pi i\alpha}$. If p is a prime number and n is an integer then we denote the least nonnegative residue of n modulo p by $r(n, p)$, i.e., $r(n, p)$ is defined by

$$r(n, p) \equiv n \pmod{p}, \qquad 0 \leqslant r(n, p) \leqslant p - 1.$$

The number of the elements of a finite set S will be denoted by $|S|$. $A, B, \ldots$ denote strictly increasing sequences of positive integers. We write

$$A(n) = \sum_{\substack{a \in A \\ a \leqslant n}} 1 \; (= |A \cap \{1, 2, \ldots, n\}|), \qquad B(n) = \sum_{\substack{b \in B \\ b \leqslant n}} 1, \ldots .$$

If the infinite sequence $B = \{b_1, b_2, \ldots\}$ is such that the equation

$$a_x - a_y = b_z \tag{1}$$

is solvable for every infinite sequence $A = \{a_1, a_2, \ldots\}$ of positive lower (asymptotic) density (i.e., B intersects the difference set of each of these

0022-314X/78/0104–0430$02.00/0

sequences A) then we say that B is a *difference intersector set*. (This terminology is due partly to R. Tijdeman.) Similarly, if

$$a_x + a_y = b_z \tag{2}$$

is solvable for every infinite sequence A of positive lower density then B is said to be a *sum intersector set*.

We shall use this terminology also for finite sequences $B \subset \{1, 2,..., N\}$. In fact, if

$$A(N) > \epsilon N \tag{3}$$

implies the solvability of (1) (if N is large in terms of ϵ) then again, B is said to be a difference intersector set. In the definition of (finite) sum intersector sets, (3) must be replaced by

$$A([N/2]) > \epsilon N.$$

Namely, if $a_u, a_v > [N/2]$ then $a_u + a_v > N$ thus B does not intersect the set of these sums $a_u + a_v$.

In [4] and [6], respectively, the second author showed that both sequences $\{1^2, 2^2,..., z^2,...\}$ and $\{2 - 1, 3 - 1, 5 - 1,..., p - 1,...\}$ form difference intersector sets. More exactly, he proved that

$$A(N) > c_1 N \frac{(\log \log N)^{2/3}}{(\log N)^{1/3}}$$

implies the solvability of

$$a_x - a_y = z^2$$

(where $z > 0$) and

$$A(N) > c_2 N \frac{(\log \log \log N)^3 \log \log \log \log N}{(\log \log N)^2}$$

implies the solvability of

$$a_u - a_v = p - 1$$

(both for large N).

In this series, we are going to continue the investigation of difference and sum intersector sets. In particular, in this paper we will discuss the case when the intersector set is well distributed simultaneously among and within all residue classes of small moduli.

In Section 2, we will prove two general theorems, saying essentially that if a sequence B is well distributed among and within all residue classes of small moduli, then it must be both difference and sum intersector set.

In Sections 3 and 4, we will apply these general theorems to investigate the solvability of the equations

$$\left(\frac{a_x - a_y}{p}\right) = +1, \qquad \left(\frac{a_u - a_v}{p}\right) = -1$$

and

$$\left(\frac{a_r + a_s}{p}\right) = +1, \qquad \left(\frac{a_t + a_z}{p}\right) = -1$$

for "large" sets $\{a_1, a_2, \ldots\}$ of residues modulo p.

Finally, in Section 5, we will apply Theorems 1 and 2 to show that in a well defined sense, "almost all" subsets of $\{1, 2, \ldots, N\}$ form both difference and sum intersector sets.

2

In this section, we will prove the following two theorems:

THEOREM 1. *Let N be a positive integer, and let $A = \{a_1, a_2, \ldots\} \subset \{1, 2, \ldots, N\}$, $B = \{b_1, b_2, \ldots\} \subset \{1, 2, \ldots, N\}$. For $0 \leqslant \alpha \leqslant 1$, we write*

$$G(\alpha) = \sum_{j=1}^{B(N)} e(b_j \alpha), \tag{4}$$

$$D(\alpha) = G(\alpha) - \frac{B(N)}{N} \sum_{n=1}^{N} e(n\alpha) \tag{5}$$

and

$$M = \max_{0 \leqslant \alpha \leqslant 1} |D(\alpha)|. \tag{6}$$

Then

$$A(N) > 3 \max\left\{M \frac{N}{B(N)}, 1\right\} \tag{7}$$

implies the solvability of the equation (1).

THEOREM 2. *Let N be a positive integer, and let $A = \{a_1, a_2, \ldots\} \subset \{1, 2, \ldots, [N/2]\}$, $B = \{b_1, b_2, \ldots\} \subset \{1, 2, \ldots, N\}$. Define $G(\alpha)$, $D(\alpha)$ and M by* (4), (5) *and* (6). *Then*

$$A([N/2]) > 2 \frac{N}{B(N)} \max\{M, 2\} \tag{8}$$

implies the solvability of the equation

$$a_x + a_y = b_z, \qquad x \neq y. \tag{9}$$

(The condition $x \neq y$ does not play an essential role; however, in some cases, we may need this restriction.)

Proof of Theorem 1. Let us write

$$F(\alpha) = \sum_{j=1}^{A(N)} e(a_j\alpha).$$

Then

$$E = \int_0^1 |F(\alpha)|^2 G(\alpha)\, d\alpha = \int_0^1 F(-\alpha) F(\alpha) G(\alpha)\, d\alpha$$

$$= \int_0^1 \sum_{x=1}^{A(N)} e(-a_x\alpha) \sum_{y=1}^{A(N)} e(a_y\alpha) \sum_{z=1}^{B(N)} e(b_z\alpha)\, d\alpha$$

$$= \sum_{x=1}^{A(N)} \sum_{y=1}^{A(N)} \sum_{z=1}^{B(N)} \int_0^1 e((-a_x + a_y + b_z)\alpha)\, d\alpha = \sum_{\substack{x,y,z \\ -a_x+a_y+b_z=0}} 1$$

Thus to prove the solvability of (1), it suffices to show that

$$E > 0. \tag{10}$$

By (7), and using the Parseval formula, we obtain that

$$E = \int_0^1 |F(\alpha)|^2 \frac{B(N)}{N} \sum_{n=1}^{N} e(n\alpha)\, d\alpha$$

$$+ \int_0^1 |F(\alpha)|^2 \left(G(\alpha) - \frac{B(N)}{N} \sum_{n=1}^{N} e(n\alpha)\right) d\alpha$$

$$= \frac{B(N)}{N} \int_0^1 \sum_{x=1}^{A(N)} e(-a_x\alpha) \sum_{y=1}^{A(N)} e(a_y\alpha) \sum_{n=1}^{N} e(n\alpha)\, d\alpha + \int_0^1 |F(\alpha)|^2 D(\alpha)\, d\alpha$$

$$= \frac{B(N)}{N} \sum_{x=1}^{A(N)} \sum_{y=1}^{A(N)} \sum_{n=1}^{N} \int_0^1 e((-a_x + a_y + n)\alpha)\, d\alpha + \int_0^1 |F(\alpha)|^2 D(\alpha)\, d\alpha$$

$$\geqslant \frac{B(N)}{N} \sum_{\substack{1 \leqslant x,y \leqslant A(N) \\ 1 \leqslant n \leqslant N \\ a_x - a_y = n}} 1 - \int_0^1 |F(\alpha)|^2 |D(\alpha)|\, d\alpha$$

$$\geqslant \frac{B(N)}{N} \sum_{1\leqslant y<x\leqslant A(N)} 1 - M\int_0^1 |F(\alpha)|^2\, d\alpha$$

$$= \frac{B(N)}{N}\binom{A(N)}{2} - MA(N) = A(N)\left(\frac{B(N)}{N}\cdot\frac{A(N)-1}{2} - M\right)$$

$$> A(N)\left(\frac{B(N)}{N}\cdot\frac{A(N)}{3} - M\right) > A(N)\left(\frac{B(N)}{N}\cdot M\frac{N}{B(N)} - M\right) = 0,$$

which proves (10) and the proof of Theorem 1 is completed.

Proof of Theorem 2. We start out from the integral

$$E_+ = \int_0^1 F^2(\alpha)\, G(-\alpha)\, d\alpha \qquad \text{with} \qquad F(\alpha) = \sum_{j=1}^{A([N/2])} e(a_j\alpha)$$

and we proceed in the same way as in the proof of Theorem 1. We obtain that

$$E_+ = \sum_{\substack{x,y,z\\ a_x+a_y=b_z}} 1$$

$$\geqslant \frac{B(N)}{N} \sum_{\substack{1\leqslant y,x\leqslant A([N/2])\\ 1\leqslant n\leqslant N\\ a_x+a_y=n}} 1 - \int_0^1 |F^2(\alpha)|\,|D(\alpha)|\, d\alpha$$

$$\geqslant \frac{B(N)}{N}(A([N/2]))^2 - M\int_0^1 |F(\alpha)|^2\, d\alpha$$

$$= \frac{B(N)}{N}(A([N/2]))^2 - MA([N/2]).$$

Hence, with respect to (8),

$$\sum_{\substack{x,y,z\\ x\neq y\\ a_x+a_y=b_z}} 1 = \sum_{\substack{x,y,z\\ a_x+a_y=b_z}} 1 - \sum_{\substack{x,z\\ 2a_x=b_z}} 1$$

$$\geqslant \left\{\frac{B(N)}{N}(A([N/2]))^2 - MA([N/2])\right\} - 2A([N/2])$$

$$= A([N/2])\left(\frac{B(N)}{N}A([N/2]) - M - 2\right) > 0$$

which proves the solvability of (9).

3

In this section, we will apply Theorems 1 and 2 to prove the following two theorems:

THEOREM 3. *Let $p > 2$ be any prime number, and let $A = \{a_1, a_2, \ldots\} \subset \{1, 2, \ldots, p-1\}$,*

$$A(p-1) > 6p^{7/8}(\log p)^{1/2}. \tag{11}$$

Then both equations

$$(a_x - a_y/p) = +1 \tag{12}$$

and

$$(a_u - a_v/p) = -1 \tag{13}$$

are solvable.

THEOREM 4. *Let $p > 2$ be any prime number, and let $A = \{a_1, a_2, \ldots\} \subset \{1, 2, \ldots, p-1\}$,*

$$A(p-1) > 16p^{7/8}(\log p)^{1/2}. \tag{14}$$

Then both equations

$$(a_x + a_y/p) = +1, \qquad x \neq y \tag{15}$$

and

$$(a_u + a_v/p) = -1, \qquad u \neq v \tag{16}$$

are solvable.

Proof of Theorem 3. Throughout the proof, we use the same notations as in Theorem 1. We put $N = p - 1$, and B in Theorem 1 will be chosen as the set of the integers n such that $1 \leqslant n \leqslant p-1$ and $(n/p) = +1$.

In order to apply Theorem 1, we have to estimate M. Obviously, for any $0 \leqslant \alpha \leqslant 1$,

$$D(\alpha) = G(\alpha) - \frac{B(N)}{N} \sum_{n=1}^{N} e(n\alpha)$$

$$= \sum_{\substack{1 \leqslant b \leqslant p-1 \\ (b/p)=+1}} e(b\alpha) - \frac{1}{2} \sum_{n=1}^{p-1} e(n\alpha) = \frac{1}{2} \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e(x\alpha).$$

Hence,

$$|D(\alpha)|^2 = D(\alpha)\, D(-\alpha)$$

$$= \frac{1}{4} \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) e(x\alpha)\, e(-y\alpha)$$

$$= \frac{1}{4} \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} \left(\frac{xy}{p}\right) e((x-y)\alpha)$$

$$= \frac{1}{4} \sum_{t=-(p-2)}^{p-2} \left\{ \sum_{\substack{1 \leqslant y \leqslant p-1 \\ 1 \leqslant t+y \leqslant p-1}} \left(\frac{(t+y)\, y}{p}\right) \right\} e(t\alpha)$$

$$= \frac{1}{4} \sum_{t=-(p-2)}^{p-2} \left\{ \sum_{\max\{1-t,1\} \leqslant y \leqslant \min\{p-t-1,\, p-1\}} \left(\frac{y^2 + ty}{p} \right) \right\} e(t\alpha)$$

$$\leqslant \frac{1}{4} \sum_{1 \leqslant y \leqslant p-1} \left(\frac{y^2}{p} \right) + \frac{1}{4} \sum_{\substack{|t| \leqslant p-2 \\ t \neq 0}} \left| \sum_{\max\{1-t,1\} \leqslant y \leqslant \min\{p-t-1,\, p-1\}} \left(\frac{y^2 + ty}{p} \right) \right|$$

$$= \frac{p-1}{4} + \frac{1}{4} \sum_{\substack{|t| \leqslant p-2 \\ t \neq 0}} \left| \sum_{\max\{1-t,1\} \leqslant y \leqslant \min\{p-t-1,\, p-1\}} \left(\frac{y^2 + ty}{p} \right) \right|. \quad (17)$$

We need the following lemma:

LEMMA 1. *Let $p > 2$ be a prime number. Let a, b, c, R, and Q be integers, such that*

$$(a, p) = 1, \quad (b^2 - 4ac, p) = 1 \qquad \text{and} \qquad 0 < R < R + Q < p. \quad (18)$$

Let

$$T = \sum_{x=R}^{R+Q-1} \left(\frac{ax^2 + bx + c}{p} \right).$$

Then

$$|T| < \tfrac{3}{2} p^{3/4} \log p.$$

For this lemma and its proof, see I. M. Vinogradov [8, Chap. VI, Problem 15].

To estimate the inner sum in (17), we apply Lemma 1 with $a = 1$, $b = t$, $c = 0$, $R = \max\{1 - t, 1\}$, $Q = \min\{p - t - 1, p - 1\} - \max\{1 - t, 1\} + 1$. Then (18) holds trivially (with respect to $-p < t < p$, $t \neq 0$). Thus we obtain from (17) that

$$|D(\alpha)|^2 < \frac{p-1}{4} + \frac{1}{4} \sum_{\substack{|t| \leqslant p-2 \\ t \neq 0}} \frac{3}{2} p^{3/4} \log p$$

$$= \frac{p-1}{4} + \frac{3}{8} \cdot 2(p-2)\, p^{3/4} \log p < \frac{p}{4} + \frac{3}{4} p^{7/4} \log p < p^{7/4} \log p.$$

Hence

$$M = \max_{0 \leqslant \alpha \leqslant 1} |D(\alpha)| < (p^{7/4} \log p)^{1/2} < p^{7/8} (\log p)^{1/2}. \quad (19)$$

Thus the right hand side of (7):

$$3 \max \left\{ M \frac{N}{B(N)}, 1 \right\} \leqslant 3 \max\{p^{7/8} (\log p)^{1/2} \cdot 2, 1\}$$

$$= 6p^{7/8} (\log p)^{1/2}. \quad (20$$

(11) and (20) yield (7). Thus we may apply Theorem 1, and we find that (1) is solvable. In other words, there exist $a_x, a_y(\in A)$ such that $a_x - a_y \in B$, i.e.,

$$\left(\frac{a_x - a_y}{p}\right) = +1,$$

which proves the solvability of (12).

The second half of the theorem (the solvability of (13)) follows from the first half of it. Namely, let d denote a fixed integer such that $(d/p) = -1$. Then applying the first half of the theorem with the sequence $\{r(da_1, p), r(da_2, p),...\}$ in place of A, we obtain the solvability of

$$+1 = \left(\frac{r(da_u, p) - r(da_v, p)}{p}\right) = \left(\frac{da_u - da_v}{p}\right) = \left(\frac{d}{p}\right)\left(\frac{a_u - a_v}{p}\right)$$

$$= -\left(\frac{a_u - a_v}{p}\right)$$

and the proof of Theorem 3 is completed.

Proof of Theorem 4. (14) implies that either

$$A\left(\frac{p-1}{2}\right) > 8p^{7/8}(\log p)^{1/2} \tag{21}$$

or

$$A(p-1) - A\left(\frac{p-1}{2}\right) > 8p^{7/8}(\log p)^{1/2}. \tag{22}$$

Assume at first that (21) holds. Let us define N and B in the same way as in the proof of Theorem 3. Then (19) holds. (19) and (21) yield that

$$A\left(\frac{p-1}{2}\right) = A(N/2) > 8M = 4\frac{p-1}{(p-1)/2}M = 4\frac{N}{B(N)}M > 2\frac{N}{B(N)}M$$

and

$$A\left(\frac{p-1}{2}\right) = A(N/2) > 8p^{7/8}(\log p)^{1/2} > 8 = 2\frac{N}{B(N)} \cdot 2.$$

Thus Theorem 2 is applicable. We obtain that (9) is solvable. In other words, there exist $a_x, a_y(\in A)$ such that $x \neq y$ and $a_x + a_y \in B$, i.e., (15) holds.

Now we are going to show that (16) is also solvable.

Let $N = p - 1$, and let B_0 denote the set of those integers n for which $1 \leqslant n \leqslant p - 1$ and $(n/p) = -1$. Let

$$G_0(\alpha) = \sum_{b \in B_0} e(b\alpha),$$

$$D_0(\alpha) = G_0(\alpha) - \frac{B_0(N)}{N} \sum_{n=1}^{N} e(n\alpha)$$

and

$$M_0 = \max_{0 \leqslant \alpha \leqslant 1} |D_0(\alpha)|$$

(while B, $G(\alpha)$, $D(\alpha)$, and M are defined in the same way as in the proof of Theorem 3). Then

$$D_0\,\alpha) = G_0(\alpha) - \frac{B_0(N)}{N} \sum_{n=1}^{N} e(n\alpha)$$

$$= \sum_{\substack{1 \leqslant n \leqslant p-1 \\ (n/p)=-1}} e(n\alpha) - \frac{1}{2} \sum_{n=1}^{p-1} e(n\alpha)$$

$$= \frac{1}{2} \sum_{n=1}^{p-1} e(n\alpha) - \sum_{\substack{1 \leqslant n \leqslant p-1 \\ (n/p)=+1}} e(n\alpha)$$

$$= \frac{B(N)}{N} \sum_{n=1}^{N} e(n\alpha) - G(\alpha) = -D(\alpha).$$

Thus

$$|D_0(\alpha)| = |D(\alpha)|. \tag{23}$$

(19), (21) and (23) yield that

$$M_0 = \max_{0 \leqslant \alpha \leqslant 1} |D_0(\alpha)| = \max_{0 \leqslant \alpha \leqslant 1} |D(\alpha)| < p^{7/8}(\log p)^{1/2}$$

$$< \frac{1}{8} A\left(\frac{p-1}{2}\right) = \frac{1}{8} A(N/2).$$

Hence

$$A(N/2) > 8M_0 = 4\frac{p-1}{(p-1)/2} M_0 = 4\frac{N}{B_0(N)} M_0 > 2\frac{N}{B_0(N)} M_0$$

and

$$A(N/2) > 8p^{7/8}(\log p)^{1/2} > 8 = 2\frac{N}{B_0(N)} \cdot 2.$$

Thus Theorem 2 is applicable (with B_0 in place of B). We obtain the solvability of $a_u + a_v \in B_0$, $u \neq v$, i.e., (16).

Finally, if (22) holds, then let A_1 denote the set of those integers which can be written in form $p - a_i$ where $N/2 < a_i \leqslant N$. Then $A_1 \subset \{1, 2,..., N/2\}$ and by (22),

$$A_1(N/2) = A(N) - A(N/2) > 8p^{7/8}(\log p)^{1/2}.$$

Thus (21) holds with A_1 in place of A. Hence, by the first part of the proof, there exist a_x, a_y, a_u, a_v such that $p - a_x$, $p - a_y$, $p - a_u$, $p - a_v \in A_1$, $x \neq y$, $u \neq v$ and

$$\left(\frac{(p - a_x) + (p - a_y)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a_x + a_y}{p}\right) = +1,$$

$$\left(\frac{(p - a_u) + (p - a_v)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a_u + a_v}{p}\right) = -1.$$

This proves that both (15) and (16) are solvable also in case (22) and the proof of Theorem 4 is completed.

4

In this section, we will investigate how far Theorems 3 and 4 are from the best possible.

Assume that $p \equiv 1 \pmod 4$ and Theorem 3 is true with $f(p)$ on the right-hand side of (11), i.e., for

$$A(p - 1) > f(p).$$

This implies that the set $A = \{1, 2,..., [f(p)] + 1\}$ contains some integers $(1 \leqslant) u < v (\leqslant [f(p)] + 1)$ such that $(v - u/p) = -1$. Here $1 \leqslant v - u \leqslant [f(p)]$, thus the least quadratic nonresidue modulo p must be less than $f(p)$. Hence, at the present time, it is hopeless to prove Theorem 3 with $O(p^\epsilon)$ on the right side of (11). (In Theorem 4, the situation is similar.)

On the other hand, in [5], the second author proved the following estimate from the opposite side:

THEOREM 5. *If p is a prime number satisfying*

$$p \equiv 1 \pmod 4$$

then there exists a set $A = \{a_1, a_2,..., a_k\} \subset \{1, 2,..., p - 1\}$ such that

$$k = A(p - 1) = \left[\frac{\log(p - 1)}{\log 4} + 1\right] \tag{24}$$

and

$$\left(\frac{a_x - a_y}{p}\right) = +1$$

is not solvable.

(See [5, Lemma 2].)

Thus the right-hand side of (11) in Theorem 3 can not be replaced by, say, $\frac{1}{2}\log p$.

Theorem 5 implies also that for $p \equiv 1 \pmod 4$, there exists a set $A^* \subset \{1, 2, \ldots, p-1\}$ such that

$$A^*(p-1) = \left[\frac{\log(p-1)}{\log 4} + 1\right] \quad \text{and} \quad \left(\frac{a_x^* - a_y^*}{p}\right) = -1$$

is not solvable. In fact, let $A = \{a_1, a_2, \ldots, a_k\}$ be a set satisfying the conditions in Theorem 5 and let d denote any integer such that $(d/p) = -1$. Then A^* can be chosen as the set formed by the integers $r(da_1, p), r(da_2, p), \ldots, r(da_k, p)$.

Also, the method of the proof of Theorem 5 can be used to prove the analog of Theorem 5 with $(a_x + a_y/p)$ in place of $(a_x - a_y/p)$.

THEOREM 6. *For any prime number $p > 2$, there exists a set $A \subset \{1, 2, \ldots, p-1\}$ such that* (24) *holds and*

$$\left(\frac{a_x + a_y}{p}\right) = +1, \qquad x \neq y \tag{25}$$

is not solvable.

Proof of Theorem 6. Let us define the graph G_{p-1} of $p-1$ vertices $Q_1, Q_2, \ldots, Q_{p-1}$ in the following way:

The vertices Q_i, Q_j (where $1 \leqslant i < j \leqslant p-1$) are connected if and only if

$$(i + j/p) = -1.$$

By a Ramsey-type theorem of Erdös and Szekeres (see [1]), if k is a positive integer satisfying

$$p - 1 \geqslant \binom{2k-2}{k-1}, \tag{26}$$

then either G_{p-1} or its complement contains a complete subgraph of k vertices. We are going to show that (26) holds with

$$k = \left[\frac{\log(p-1)}{\log 4} + 1\right]. \tag{27}$$

In fact,

$$2^{2k-2} = 2^{2[\log(p-1)/\log 4+1]-2} \leqslant 2^{2\log(p-1)/\log 4} = p - 1.$$

Combining this with the trivial inequality

$$\binom{2k-2}{k-1} \leqslant 2^{2k-2},$$

we obtain (26). Thus the theorem of Erdos and Szekeres can be applied with the k given in (27).

Assume at first that G_{p-1} contains a complete subgraph of k vertices; denote its vertices by $Q_{i_1}, Q_{i_2},..., Q_{i_k}$. Then obviously, the set $A = \{i_1, i_2,..., i_k\}$ satisfies (24) and (25) is not solvable.

Assume now that the complement of G_{p-1} contains a complete subgraph of k vertices. Let us denote the vertices of this subgraph by $Q_{j_1}, Q_{j_2},..., Q_{j_k}$, and let d denote any integer satisfying $(d/p) = -1$. Then it is easy to see that the set A in Theorem 6 can be chosen as the set formed by the integers $r(dj_1, p), r(dj_2, p),..., r(dj_k, p)$.

Again, it can be shown easily that the statement of Theorem 6 remains valid with

$$\left(\frac{a_u + a_v}{p}\right) = -1, \qquad u \neq v,$$

in place of (25).

5

If k, N are positive integers such that $1 \leqslant k \leqslant N$ then let $\Gamma(N, k)$ denote the set of those sets B for which $B \subset \{1, 2,..., N\}$ and $|B| = k$ hold. In this section, we will show that for

$$N^c < k < N, \tag{28}$$

"almost all" sets $B \in \Gamma(N, k)$ form both difference and sum intresector sets. (Note that on the other hand, there exist relatively many sets $B \subset \{1, 2,..., N\}$ which are neither difference nor sum intersector sets; in fact, if $B \subset \{1, 3,..., 2k + 1,..., 2[N - 1/2] + 1\}$ then B is neither difference nor sum intersector set.)

We remark that replacing (28) by the slightly weaker

$$N^{1-\epsilon_N} < k < N \qquad \text{where } \epsilon_N \to 0_+ \text{ arbitrary slowly,} \tag{29}$$

and in case of difference intersector sets, this statement can be proved also in an elementary way, relatively easily. In fact, (29) implies that for almost all $B \in \Gamma(N, k)$, B contains an arithmetic progression of form $d, 2d,..., td$ where

$t = t(\epsilon_N) \to +\infty$ as $\epsilon_N \to 0$. But it can be shown easily that such a set B is a difference intersector set.

For $B \in \Gamma(N, k)$, we write

$$\sum_{\substack{j \leqslant n \\ j \equiv m \pmod q \\ j \in B}} 1 - \frac{B(N)}{N} \sum_{\substack{j \leqslant n \\ j \equiv m \pmod q}} 1$$

$$= \sum_{\substack{j \leqslant n \\ j \equiv m \pmod q \\ j \in B}} 1 - \frac{k}{N} \sum_{\substack{j \leqslant n \\ j \equiv m \pmod q}} 1 = h_{(m,q)}(B, n)$$

and

$$\max_{\substack{1 \leqslant m \leqslant q \\ 1 \leqslant n \leqslant N}} |h_{(m,q)}(B, n)| = H_q(B). \tag{30}$$

THEOREM 7. *Let k, N be positive integers, satisfying*

$$N^{2/3} \log N < k \leqslant N. \tag{31}$$

If N is large enough then for all but $(1/N^2)\binom{N}{k}$ sets $B \in \Gamma(N, k)$, the conditions

$$A \subset \{1, 2, \ldots, N\} \quad \text{and} \quad \frac{A(N)}{N} > 2400 \left(\frac{N^{2/3} \log N}{k}\right)^{1/2} \tag{32}$$

imply the solvability of Eq. (1).

THEOREM 8. *Let k, N be positive integers, satisfying* (31). *If N is large enough then for all but $(1/N^2)\binom{N}{k}$ sets $B \in \Gamma(N, k)$, the conditions*

$$A \subset \{1, 2, \ldots, [N/2]\} \quad \text{and} \quad \frac{A([N/2])}{N} > 1600 \left(\frac{N^{2/3} \log N}{k}\right)^{1/2} \tag{33}$$

imply the solvability of Eq. (9).

(Note that if $k/N^{2/3} \log N \to +\infty$, then for large N, $A(N) > \epsilon N$, respectively $A([N/2]) > \epsilon N$, implies that (31) and (32) hold. Thus in this case, almost all sets $B \in \Gamma(N, k)$ are simultaneously difference and sum intersector sets.)

We shall need two lemmas.

LEMMA 2. *If the positive integers k, N satisfy* (31) *then for all but $(1/N^2)\binom{N}{k}$ sets $B \in \Gamma(N, k)$, we have*

$$H_q(B) < 100 \left(\frac{k}{q} \log N\right)^{1/2} \tag{34}$$

for all $1 \leqslant q \leqslant N^{2/3}$.

Proof of Lemma 2. We use the same method as in [7]. Let Δ denote the set of those sets $B \in \Gamma(N, k)$ for which

$$H_q(B) \geqslant 100 \left(\frac{k}{q} \log N\right)^{1/2}$$

holds for some q with

$$1 \leqslant q \leqslant N^{2/3}. \tag{35}$$

In other words,

$$|\, h_{(m,q)}(B, n)| \geqslant 100 \left(\frac{k}{q} \log N\right)^{1/2} \tag{36}$$

for some q, m, n with

$$1 \leqslant m \leqslant q, \qquad 1 \leqslant n \leqslant N. \tag{37}$$

Let $\Delta(q, m, n)$ denote the set of those sets $B \in \Delta$, for which (36) holds for some q, m, n, satisfying (35) and (37). Then

$$\Delta \subset \bigcup_{\substack{1 \leqslant q \leqslant N^{2/3} \\ 1 \leqslant m \leqslant q \\ 1 \leqslant n \leqslant N}} \Delta(q, m, n);$$

hence

$$|\, \Delta \,| \leqslant \sum_{q=1}^{[N^{2/3}]} \sum_{m=1}^{q} \sum_{n=1}^{N} |\, \Delta(q, m, n)|. \tag{38}$$

Thus in order to estimate $|\, \Delta \,|$, we have to estimate $|\, \Delta(q, m, n)|$.

Let us fix q, m, n and let $B \in \Delta(q, m, n)$. Let

$$B = B_1 \cup B_2,$$

where

$$B_1 \subset \left\{m, m + q, \ldots, m + \left[\frac{n - m}{q}\right] q\right\}$$

and

$$B_2 \cap \left\{m, m + q, \ldots, m + \left[\frac{n - m}{q}\right] q\right\} = \varnothing.$$

Let us write

$$\sum_{\substack{j \leqslant n \\ j \equiv m (\mathrm{mod}\ q) \\ j \in B}} 1 = u$$

and

$$\sum_{\substack{j \leqslant n \\ j \equiv m (\mathrm{mod}\ q)}} 1 = \left[\frac{n - m}{q}\right] + 1 = t.$$

Then

$$[n/q] \leqslant t \leqslant [n/q] + 1, \tag{39}$$

by (36),

$$\left| u - \frac{k}{N} t \right| \geqslant 100 \left(\frac{k}{q} \log N \right)^{1/2}, \tag{40}$$

and with respect to $B \in \Gamma(N, k)$,

$$|B_2| = |B| - |B_1| = k - u. \tag{41}$$

For fixed u (and m, n, q), B_1 can be chosen from the t integers in $\{m, m+q,\ldots, m+(t-1)q\}$, thus it can be chosen in at most $\binom{t}{u}$ ways. Similarly, B_2 can be chosen from the $N-t$ integers in $\{1, 2,\ldots, N\} - \{m, m+q,\ldots, m+(t-1)q\}$ thus with respect to (41), it can be chosen in at most $\binom{N-t}{k-u}$ ways. Summarizing, we find that for fixed u, B can be chosen in at most $\binom{t}{u}\binom{N-t}{k-u}$ ways. Thus with respect to (40),

$$\begin{aligned} |\Delta(q, m, m)| &\leqslant \sum_{\substack{u \\ |u-(k/N)t| \geqslant 100((k/q)\log N)^{1/2}}} \binom{t}{u}\binom{N-t}{k-u} \\ &= \sum_{u \leqslant (k/N)t - 100((k/q)\log N)^{1/2}} \binom{t}{u}\binom{N-t}{k-u} \\ &\quad + \sum_{u \geqslant (k/N)t + 100((k/q\log N)^{1/2}} \binom{t}{u}\binom{N-t}{k-u} = \Sigma_1 + \Sigma_2 . \end{aligned} \tag{42}$$

Let us write

$$F(u) = \binom{t}{u}\binom{N-t}{k-u}.$$

First we estimate Σ_1. Let $(k/N)t - u = d$. Then for $d \geqslant 0$, $u \geqslant 0$, we have

$$\begin{aligned} \frac{F(u-1)}{F(u)} &= \frac{t!\,(N-t)!}{(u-1)!\,(t-u+1)!\,(k-u+1)!\,(N-t-k+u-1)!} \\ &\quad \cdot \frac{u!\,(t-u)!\,(k-u)!\,(N-t-k+u)!}{t!\,(N-t)!} \\ &= \frac{u'N-t-k+u)}{(t-u+1)(k-u+1)} = 1 - \frac{tk - uN + k + t - 2u + 1}{(t-u+1)(k-u+1)} \\ &= 1 - \frac{dN + (k-u) + (t-u) + 1}{(t-u+1)(k-u+1)} \leqslant 1 - \frac{dN}{(t+1)(k+1)} \\ &\leqslant 1 - \frac{dN}{4tk} (\leqslant 1), \end{aligned} \tag{43}$$

since $k-u \geqslant 0$, $t-u \geqslant 0$ follow from $d=(kt/N)-u \geqslant 0$. Let us put $r_1=[kt/n]$ and

$$s_1=\left[\frac{k}{N}t-100\left(\frac{k}{q}\log N\right)^{1/2}\right] \leqslant r_1+1-\left[100\left(\frac{k}{q}\log N\right)^{1/2}\right]. \quad (44)$$

Then by (43), we have

$$F(s_1)=F(r_1)\prod_{u=s_1+1}^{r_1}\frac{F(u-1)}{F(u)} \leqslant F(r_1)\prod_{u=s_1+1}^{r_1}\left(1-\frac{\left(\frac{kt}{N}-u\right)N}{4tk}\right)$$

for $s_1 \geqslant 0$. Writing $u=r_1-j$:

$$\begin{aligned}
F(s_1) &\leqslant F(r_1)\prod_{j=0}^{r_1-s_1-1}\left(1-\frac{\left(\frac{kt}{N}-r_1\right)N+jN}{4tk}\right)\\
&\leqslant F(r_1)\prod_{j=0}^{r_1-s_1-1}\left(1-\frac{jN}{4tk}\right) \leqslant F(r_1)\exp\left\{-\sum_{j=0}^{r_1-s_1-1}\frac{jN}{4tk}\right\}\\
&= F(r_1)\exp\left\{-\frac{N}{4tk}\cdot\frac{(r_1-s_1-1)(r_1-s_1)}{2}\right\}\\
&\leqslant F(r_1)\exp\left\{-\frac{N}{8tk}(r_1-s_1-1)^2\right\} \qquad (45)
\end{aligned}$$

since $1-x \leqslant e^{-x}$ for $x \geqslant 0$. By (35), (37), and (39), we have

$$t \leqslant \left[\frac{n}{q}\right]+1 \leqslant \frac{N}{q}+1 \leqslant \frac{N}{q}+\frac{1}{4}N^{1/3} \leqslant \frac{5}{4}\frac{N}{q} \qquad (46)$$

for $N \geqslant 4^3$. Furthermore, by (31) and (35),

$$\left(\frac{k}{q}\log N\right)^{1/2} > \left(\frac{N^{2/3}\log N}{N^{2/3}}\log N\right)^{1/2} = \log N, \qquad (47)$$

thus with respect to (44) and (46),

$$\begin{aligned}
\frac{N}{8tk}(r_1-s_1-1)^2 &> \frac{N}{8\cdot\frac{5}{4}\frac{N}{q}\cdot k}\left(\left[100\left(\frac{k}{q}\log N\right)^{1/2}\right]-2\right)^2\\
&> \frac{q}{10k}\left\{50\left(\frac{k}{q}\log N\right)^{1/2}\right\}^2 = 250\log N
\end{aligned}$$

for large N. Putting this into (45), we obtain that

$$F(s_1) < F(r_1)\exp\{-250\log N\} = \frac{1}{N^{250}}F(r_1).$$

Thus for large N,

$$\Sigma_1 = \sum_{u=0}^{s_1} F(u) \leqslant (s_1+1)F(s_1) \leqslant \frac{k}{N}t\cdot\frac{1}{N^{250}}F(r_1)$$

$$< \frac{1}{N^{249}}F(r_1) < \frac{1}{N^{249}}\sum_{u=0} F(u) = \frac{1}{N^{249}}\binom{N}{k}$$

(since $F(u)$ is increasing for $0 \leqslant u \leqslant s_1$, by (43)).

Σ_2 can be estimated similarly. Let $e = u - (k/N)t$. Then for $e \geqslant 0$, $u \leqslant t$, $u \leqslant k$, $k - u \leqslant N - t$, we have

$$\frac{F(u+1)}{F(u)} = \frac{(t-u)(k-u)}{(u+1)(N-t-k+u+1)}$$

$$= 1 - \frac{eN + (N-t-k+u+1) + u}{(u+1)(N-t-k+u+1)}$$

$$< 1 - \frac{eN}{2u\cdot 3N} = 1 - \frac{e}{6u} \tag{49}$$

(obviously, $0 < 1 - e/6u \leqslant 1$).

Let us put $r_2 = [(k/N)t] + 1$ and define the integer s_2 by

$$s_2 - 1 < \frac{k}{N}t + 100\left(\frac{k}{q}\log N\right)^{1/2} \leqslant s_2 .$$

Obviously,

$$s_2 \geqslant r_2 - 1 + 100\left(\frac{k}{q}\log N\right)^{1/2} \tag{50}$$

and with respect to (31), (35), (37), and (39),

$$s_2 - 1 < \frac{k}{N}t + 100\left(\frac{k}{q}\log N\right)^{1/2} \leqslant \frac{k}{N}\left(\left[\frac{n}{q}\right]+1\right) + 100\left(\frac{k}{q}\log N\right)^{1/2}$$

$$\leqslant \frac{k}{N}\cdot\frac{2N}{q} + 100\left(\frac{k}{q}\log N\right)^{1/2} = 2\frac{k}{q}\left(1 + 50\left(\frac{q}{k}\log N\right)^{1/2}\right)$$

$$\leqslant 2\frac{k}{q}\left(1 + 50\left(\frac{N^{2/3}\log N}{k}\right)^{1/2}\right) < 102\frac{k}{q}. \tag{51}$$

By (47), (49), (50), and (51), we have

$$F(s_2) = F(r_2) \prod_{u=r_2}^{s_2-1} \frac{F(u+1)}{F(u)} < F(r_2) \prod_{u=r_2}^{s_2-1} \left(1 - \frac{u - \frac{k}{N}t}{6u}\right)$$

$$= F(r_2) \prod_{j=0}^{s_2-r_2-1} \left(1 - \frac{\left(r_2 - \frac{k}{N}t\right) + j}{6(r_2+j)}\right) < F(r_2) \prod_{j=0}^{s_2-r_2-1} \left(1 - \frac{j}{6(r_2+j)}\right)$$

$$< F(r_2) \exp\left\{-\frac{1}{6} \sum_{j=0}^{s_2-r_2-1} \frac{j}{r_2+j}\right\} < F(r_2) \exp\left\{-\frac{1}{6} \sum_{j=0}^{s_2-r_2-1} \frac{j}{s_2-1}\right\}$$

$$= F(r_2) \exp\left\{-\frac{1}{6} \cdot \frac{1}{s_2-1} \frac{(s_2-r_2-1)(s_2-r_2)}{2}\right\}$$

$$< F(r_2) \exp\left\{-\frac{1}{12} \frac{1}{s_2-1} (s_2-r_2-1)^2\right\}$$

$$\leqslant F(r_2) \exp\left\{-\frac{1}{12} \cdot \frac{1}{102\frac{k}{q}} \cdot \left(100\left(\frac{k}{q}\log N\right)^{1/2} - 2\right)^2\right\}$$

$$< F(r_2) \exp(-8 \log N) = \frac{1}{N^8} F(r_2).$$

Thus for large N,

$$\Sigma_2 = \sum_{u=s_2}^{t} F(u) \leqslant (t+1) F(s_2) < 2t \cdot \frac{1}{N^8} F(r_2)$$

$$< \frac{1}{N^6} F(r_2) \leqslant \frac{1}{N^6} \sum_{u=0}^{t} F(u) = \frac{1}{N^6} \binom{N}{k}. \tag{52}$$

Equations (42), (48), and (52) yield that for fixed q, m, n and large N,

$$|\Delta(q,m,n)| < \frac{1}{N^{249}} \binom{N}{k} + \frac{1}{N^6} \binom{N}{k} < \frac{2}{N^6} \binom{N}{k} < \frac{1}{N^5} \binom{N}{k}.$$

Thus we obtain from (38) that

$$|\Delta| \leqslant \sum_{q=1}^{[N^{2/3}]} \sum_{m=1}^{q} \sum_{n=1}^{N} |\Delta(q,m,n)| < N^3 \cdot \frac{1}{N^5} \binom{N}{k} = \frac{1}{N^2} \binom{N}{k}$$

which completes the proof of Lemma 2.

LEMMA 3. *If a, q are integers, $q \geqslant 1$, β is a real number, $B \in \Gamma(N,k)$, and*

$G(\alpha)$, $D(\alpha)$, $H_q(B)$ are defined by (4), (5), *and* (30), *respectively, then we have*

$$\left| D\left(\frac{a}{q}+\beta\right)\right| = \left| G\left(\frac{a}{q}+\beta\right) - \frac{k}{N}\sum_{j=1}^{N} e\left\{j\left(\frac{a}{q}+\beta\right)\right\}\right| < qH_q(B)(2\pi N\,|\,\beta\,|\,+1).$$

Proof of Lemma 3. For any real number α, we put

$$G_n(\alpha) = \sum_{\substack{j\leqslant n\\ j\in B}} e(j\alpha),$$

$$T_n(\alpha) = \sum_{j=1}^{n} e(j\alpha),$$

and

$$D_n(\alpha) = G_n(\alpha) - \frac{k}{N}T_n(\alpha)$$

(so that $G_N(\alpha) = G(\alpha)$ and $D_N(\alpha) = D(\alpha)$). Then for $n = 1, 2,\ldots, N$, we have

$$\begin{aligned}
\left| D_n\left(\frac{a}{q}\right)\right| &= \left| G_n\left(\frac{a}{q}\right) - \frac{k}{N}T_n\left(\frac{a}{q}\right)\right| \\
&= \left| \sum_{\substack{j\leqslant n\\ j\in B}} e\left(j\frac{a}{q}\right) - \frac{k}{N}\sum_{j=1}^{n} e\left(j\frac{a}{q}\right)\right| \\
&= \left| \sum_{m=1}^{q}\left(\sum_{\substack{j\leqslant n\\ j\equiv m(\mathrm{mod}\ q)\\ j\in B}} 1 - \frac{k}{N}\sum_{\substack{j\leqslant n\\ j\equiv m(\mathrm{mod}\ q)}} 1\right) e\left(m\frac{a}{q}\right)\right| \\
&= \left| \sum_{m=1}^{q} h_{(m,q)}(B,n)\, e\left(m\frac{a}{q}\right)\right| \leqslant \sum_{m=1}^{q} |\, h_{(m,q)}(B,n)| \\
&\leqslant \sum_{m=1}^{q} H_q(B) = qH_q(B).
\end{aligned}$$

Thus we obtain by partial summation (putting $D_0(\alpha) = 0$) that

$$\begin{aligned}
\left| D\left(\frac{a}{q}+\beta\right)\right| &= \left| D_N\left(\frac{a}{q}+\beta\right)\right| = \left| \sum_{n=1}^{N}\left(D_n\left(\frac{a}{q}\right) - D_{n-1}\left(\frac{a}{q}\right)\right) e(n\beta)\right| \\
&= \left| \sum_{n=1}^{N} D_n\left(\frac{a}{q}\right)\{e(n\beta) - e((n+1)\beta)\} + D_N\left(\frac{a}{q}\right) e((N+1)\beta)\right| \\
&\leqslant \sum_{n=1}^{N}\left| D_n\left(\frac{a}{q}\right)\right| |\,1 - e(\beta)| + \left| D_N\left(\frac{a}{q}\right)\right| \\
&\leqslant \sum_{n=1}^{N} qH_q(B)\cdot 2\pi\,|\,\beta\,| + qH_q(B) = qH_q(B)(2\pi N\,|\,\beta\,|\,+1)
\end{aligned}$$

since

$$|1 - e(\beta)| \leqslant 2\pi |\beta|$$

for every real number β and this completes the proof of Lemma 3.

Completion of the proofs of Theorems 7 and 8. Assume that a set $B \in \Gamma(N, k)$ satisfies (34) for all $1 \leqslant q \leqslant N^{2/3}$. For any real number α, there exist integers a, q such that

$$1 \leqslant q \leqslant N^{2/3},$$
$$(a, q) = 1,$$

and

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{qN^{2/3}}.$$

Thus writing $\beta = \alpha - (a/q)$, Lemma 3 yields that

$$\begin{aligned}
|D(\alpha)| &= \left|D\left(\frac{a}{q} + \beta\right)\right| < qH_q(B)(2\pi N|\beta| + 1) \\
&< q \cdot 100\left(\frac{k}{q}\log N\right)^{1/2} \cdot \left(2\pi N \frac{1}{qN^{2/3}} + 1\right) \\
&= 100\left\{2\pi\left(\frac{k}{q}\log N\right)^{1/2} N^{1/3} + (kq\log N)^{1/2}\right\} \\
&\leqslant 100\{2\pi(k\log N)^{1/2} N^{1/3} + (kN^{2/3}\log N)^{1/2}\} \\
&= 100(2\pi + 1)(kN^{2/3}\log N)^{1/2} < 800(kN^{2/3}\log N)^{1/2};
\end{aligned}$$

hence

$$M = \max_{0 \leqslant \alpha \leqslant 1} |D(\alpha)| < 800(kN^{2/3}\log N)^{1/2}.$$

This holds for all the sets $B \in \Gamma(N, k)$ satisfying (34) and by Lemma 2, (34) holds for all but $(1/N^2)\binom{N}{k}$ sets $B \in \Gamma(N, k)$ (if N is large). Thus for large N and for all but $(1/N^2)\binom{N}{k}$ sets $B \in \Gamma(N, k)$, we have

$$\begin{aligned}
3\max\left\{M\frac{N}{B(N)}, 1\right\} &\leqslant 3\max\left\{800(kN^{2/3}\log N)^{1/2}\frac{N}{k}, 1\right\} \\
&= 3\max\left\{800\left(\frac{N^{2/3}\log N}{k}\right)^{1/2} N, 1\right\} \\
&= 2400\left(\frac{N^{2/3}\log N}{k}\right)^{1/2} N \qquad (53)
\end{aligned}$$

(with respect to $k \leqslant N$) and

$$2\frac{N}{B(N)}\max\{M, 2\} \leqslant 2\frac{N}{k}\max\{800(kN^{2/3}\log N)^{1/2}, 2\}$$

$$= 1600\left(\frac{N^{2/3}\log N}{k}\right)^{1/2} N. \tag{54}$$

Combining (32) with (53), we obtain (7). Thus Theorem 1 yields the solvability of Eq. (1) which completes the proof of Theorem 7. Similarly, (8) follows from (33) and (54) thus Theorem 2 yields the solvability of (9) and this proves Theorem 8.

REFERENCES

1. P. ERDÖS AND G. SZEKERES, A combinatorial problem in geometry, *Compositio Math.* **2** (1935), 463–470.
2. K. F. ROTH, Sur quelques ensembles d'entiers, *C.R. Acad. Sci. Paris* **234** (1952), 388–390.
3. K. F. ROTH, On certain sets of integers, *J. London Math. Soc.* **28** (1953), 104–109.
4, 5, 6. A. SÁRKÖZY, On difference sets of sequences of integers, I, *Acta Math. Acad. Sci. Hungar.*, to appear; II, *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.*, to appear; and III, *Acta Math. Acad. Sci. Hungar.* to appear.
7. A. SÁRKÖZY, Some remarks concerning irregularities of distribution of sequences of integers in arithmetic progressions, II, *Studia Sci. Math. Hungar.*, to appear.
8. I. M. VINOGRADOV, "Osnovy Teorii Čisel" "Foundations of the Theory of Numbers"), 5th ed., Gosudarstvennoe Izdatel'stvo Tehniko-Teoretičeskoĭ Literatury, Moscow/ Leningrad, 1949.